REMARKS

Applicants appreciate the Examiner's attention to the above referenced application. Reconsideration of this application in view of the enclosed amendments and remarks is requested. Claims 2-7, 9-15, and 17-45 have been canceled. Claims 1, 8, and 18 have been amended. Claims 46-85 have been added. Claims 46, 58, and 71 are the pending independent claims.

ARGUMENT

The Office Action includes rejections based on 35 U.S.C. §§ 102(e) and 103(a). The Office Action also objects to the specification and asserts that the declaration does not include the signatures of all applicants.

Declaration

The present application names ten inventors (Ellison, Golliver, Herbert, Lin, McKeen, Neiger, Reneris, Sutton, Thakkar, and Mittal). Applicants' file indicates that the declaration mailed on July 27, 2000 includes signatures from all ten of those inventors. The return postcard for that filing is time stamped July 31, 2000 by the U.S.P.T.O. A copy of the declaration with signatures from all ten inventors is enclosed herewith.

Objection to the Specification

The Office Action states that a word in the application was misspelled and a sentence in the application was unclear. This response corrects the misspelled word and adds two commas to the sentence at issue, to clarify that the sentence describes an embodiment in which an "isolated bus cycle generator" exchanges an operand with an "instruction decoder and execution unit."

35 U.S.C. § 102(e)

The Office Action rejects claims 1, 3, 16, 18, 31, and 32 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,292,874 by Philip C. Barnett (hereinafter "Barnett"). To the extent that the Examiner might apply this rejection to the claims now pending, Applicants respectfully traverse.

Embodiments of the present invention include a system that supports two complementary approaches to access control: privilege rings and isolated/non-isolated execution modes. For instance, claim 46 recites a system that includes support for "a ring 0 operating mode" and a "higher ring operating mode," while also including support for an "isolated execution mode" and a "non-isolated execution mode within the ring 0 operating mode." Claims 58 and 71 also involve support for two complementary approaches to access control. For instance, claim 58 recites an "isolated execution circuit" in a processor that supports "bifurcation of the ring 0 operating mode into an isolated execution mode and a non-isolated execution mode." Claim 71 recites a method that includes an operation of receiving a configuration setting to switch a processor "between an isolated execution mode within the ring 0 operating mode and a non-isolated execution mode within the ring 0 operating mode," where the processor also supports one or more higher ring operating modes.

By contrast, Barnett discusses only a single approach to access control. Specifically, Barnett relates to a "memory management circuit for a single chip processing circuit" that provides two distinct security states: "secure kernel mode" and "application mode" (Abstract). Barnett does not disclose access control that provides for a state within a state, such as an isolated execution mode within a privilege ring. Barnett therefore does not anticipate the pending independent claims.

In addition, in the present application, the pending independent claims refer to special bus cycles that are used to support the isolated execution mode. For instance, claim 71 recites an operation of "generating isolated bus cycles with the processor executing in the isolated execution mode, wherein the isolated bus cycles enable a module to access a resource that is only accessible from the isolated execution mode of the ring 0 operating mode." Applicants can find no mention whatsoever of buses in Barnett. For these and other reasons, Barnett does not anticipate the pending independent claims.

35 U.S.C. § 103(a)

The Office Action rejects claim 2 under 35 U.S.C. § 103(a) as being unpatentable over Barnett in view of U.S. Patent No. 5,737,760 by George G. Grimmer, Jr. et al. (hereinafter "Grimmer") and U.S. Patent No. 6,499,123 by Harold L. McFarland et al. (hereinafter "McFarland"). The Office Action rejects claims 4-6 under § 103(a) as being unpatentable over Barnett in view of U.S. Patent No. 5,688,971 by E. David Neufeld (hereinafter "Neufeld"). The Office Action rejects claims 7-13 under § 103(a) as being unpatentable over Barnett in view of Neufeld and Grimmer. The Office Action rejects claims 14-15 under § 103(a) as being unpatentable over Barnett in view of Neufeld, Grimmer, and McFarland. The Office Action rejects claims 17 and 19-30, as well as 32 and 34-45 on the basis of "similar rationale" to that provided for claims 2 and 4-15. To the extent that the Examiner might apply these rejections to the claims now pending, Applicants respectfully traverse.

Like Barnett, Grimmer pertains to a single-chip processing circuit, and Grimmer discusses an approach to access control that provides for secure and non-secure operating modes (column 2, lines 28-37). McFarland and Neufeld, however, focus on technical fields other than security. McFarland relates to an integrated circuit with a normal mode for operating under normal conditions and a debug mode for operating to test and debug the integrated circuit (Abstract). Neufeld relates to an apparatus and method for performing posted disk read operations, in which a "read complete signal" is issued before the transfer of information from the disk is actually complete (Abstract).

The cited references do not provide motivation to combine those references. Furthermore, even if the cited references were to be combined, the combination would not disclose or suggest the features recited in the pending independent claims. For example, the combination would not disclose or suggest the use of an isolated execution mode within a privileged operating mode. Furthermore, the combination would not disclose or suggest the generation of isolated bus cycles to support an isolated execution mode within a privileged operating mode.

Additional Unanticipated Features

Furthermore, the independent and dependent claims in the present application recite additional features that are not disclosed or suggested by the cited art. For instance, claim 72 recites operations of "loading a processor nub into the isolated memory area, using isolated bus cycles" and "verifying an operating system nub, using the processor nub." Claim 74 recites an operation of "generating platform verification data" based on attributes including a platform key, a processor nub loaded into the isolated memory area, and an operating system nub loaded into the isolated memory area. The claims also recite many additional features that are not disclosed or suggested by the cited art.

CONCLUSION

For the reasons set forth above and other reasons readily apparent, independent claims 46, 58, and 71 are allowable. All other pending claims depend ultimately from one of the independent claims, and each therefore includes the features of its parent claim or claims. For that reason and many others, the dependent claims are also allowable. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 314-0349. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: 3/31/04

Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 314-0349

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on:

3.31.04
Date of Deposit

Derek S. Watson
Name of Person Mailing Correspondence

Signature 3.31.04 Date